Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: October 2, 2026

T. Adebayo
O. Apalowo
F. Makanjuola
Veridom Ltd

April 2, 2026

OMP Domain Profile: EU AI Act Article 12 Logging and Traceability Requirements for High-Risk AI System Operators

draft-veridom-omp-euaia-00

Abstract

This document defines a domain profile of the Operating Model Protocol (OMP) for high-risk AI system operators subject to Article 12 of Regulation (EU) 2024/1689 (the EU AI Act). Article 12 requires that high-risk AI systems automatically generate tamper-resistant logs capable of ensuring traceability throughout the system's lifetime. This profile specifies how OMP's deterministic routing invariant, Watchtower enforcement framework, and three-layer cryptographic integrity architecture (SHA-256, RFC 3161, institution signature) satisfy the Article 12 requirements, and defines the domain-specific Watchtower configurations and Audit Trace schema extensions applicable to EU high-risk AI deployments under Annex III of the Regulation.

The core OMP specification is defined in a separate Internet-Draft (\"Operating Model Protocol (OMP): A Deterministic Decision-Enforcement Protocol with Externalized Proof-of-Integrity\").

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 2, 2026.

Copyright Notice

Table of Contents

1. Introduction

Regulation (EU) 2024/1689 (the EU AI Act) [EUAIA] establishes obligations for providers and deployers of high-risk AI systems, including requirements for logging and traceability under Article 12. The Article 12 obligations apply to the Annex III categories of high-risk AI systems, including those used in:

- credit scoring and creditworthiness assessment (Annex III point 5(b));
- employment and worker management AI (Annex III point 4);
- AI systems used in education and vocational training (Annex III point 3);
- AI systems used by competent authorities (Annex III point 6);
- AI systems used in the administration of justice (Annex III point 8).

The Article 12 obligations take full effect on August 2, 2026.

The Operating Model Protocol (OMP) [I-D.veridom-omp] is a deterministic decision-enforcement protocol that classifies every interaction in a regulated operation into exactly one of three outcome states (AUTONOMOUS, ASSISTED, or ESCALATED) and generates a tamper-evident Audit Trace sealed with a three-layer cryptographic integrity architecture at the point of every decision. This architecture is designed to satisfy the Article 12 requirements structurally — through the design of the decision pipeline — rather than through retrospective reporting.

This document defines the domain-specific parameters and Watchtower configurations that instantiate OMP for EU AI Act Article 12 compliance, and specifies how the OMP Audit Trace schema extensions for this profile map to the specific logging requirements of Article 12(2).

Operators who implement OMP under this profile produce per-decision evidence records that:

- are generated automatically as an integral output of the decision pipeline (Article 12(1));

- are tamper-resistant through cryptographic sealing with a Qualified Electronic Timestamp under eIDAS Article 41 (Article 12(1));
- capture the operational period of each use with externally verifiable temporal anchoring (Article 12(2)(a));
- capture the state of all external reference databases queried at the moment of the decision (Article 12(2)(b));
- record input data in canonical form enabling decision re-verification (Article 12(2)(c));
- support decision-level traceability for post-market monitoring and supervisory examination (Article 12(3)).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] [RFC8174].

2. Terminology

This document uses the terminology defined in [I-D.veridom-omp]. In addition:

Article 12 Logging Obligation
: The requirements imposed on high-risk AI system operators by Article 12 of Regulation (EU) 2024/1689 (EU AI Act).

High-Risk AI System
: An AI system listed in Annex III of Regulation (EU) 2024/1689, or designated as high-risk by the European Commission under Article 7.

Qualified Electronic Timestamp (QTS)
: A qualified electronic timestamp as defined in Article 3(34) of Regulation (EU) 910/2014 (eIDAS), produced by a Qualified Trust Service Provider (QTSP) listed in a Member State’s trusted list under Article 22 of eIDAS.

QTSP
: Qualified Trust Service Provider. Under this profile, QTSP is used as the issuing authority for the RFC 3161 TimeStampToken required by the OMP three-layer integrity architecture.

EU AI Act Profile (EUAIA Profile)
: The domain-specific configuration of OMP defined in this document.

Post-Market Monitoring System (PMMS)
: The system required under Article 72 of the EU AI Act for providers of high-risk AI systems to collect and review data on the performance of deployed systems throughout their lifetime.

Supervisory Authority
: A national competent authority designated under Article 70 of the EU AI Act, responsible for market surveillance and enforcement.

3. EU AI Act Article 12 Requirements Analysis

Article 12 imposes six distinct technical requirements on high-risk AI system operators. This section maps each requirement to the OMP mechanism that satisfies it.

3.1. Requirement 1: Automatic generation

Article 12(1) requires that high-risk AI systems be designed and developed with capabilities enabling the automatic generation of logs.

OMP MECHANISM: The OMP Audit Trace is generated as an integral output of Stage S5 of the five-stage OMP pipeline. Stage S5 is mandatory — no interaction can complete the OMP pipeline without producing a sealed Audit Trace. The Audit Trace is not produced by a secondary logging process that reads from the primary system; it is the output of Stage S5, which executes as part of the decision pipeline itself. This satisfies the automatic generation requirement structurally, not through configuration.

Under this profile, implementations MUST NOT implement Stage S5 as an optional or configurable component. Audit Trace generation MUST be mandatory for all interactions regardless of routing outcome.

3.2. Requirement 2: Tamper resistance

Article 12(1) requires that logs have tamper-resistant capabilities to ensure traceability throughout the AI system's lifetime.

OMP MECHANISM: OMP seals every Audit Trace with a three-layer integrity architecture:

- Layer 1 (SHA-256 content hash): proves that the content of the Audit Trace record has not been altered since sealing. The records are chained in a Merkle structure; modification of any historical record invalidates all subsequent chain hashes, making deletion detectable without access to the deleted record.

- Layer 2 (RFC 3161 TimeStampToken [RFC3161] from a QTSP): proves the Audit Trace existed at a specific moment in time, attested by a party external to the operator. The QTSP's signature cannot be retroactively obtained for a fabricated or post-hoc record. Under this profile, the RFC 3161 timestamp MUST be obtained from a QTSP listed in an EU Member State trusted list under eIDAS Article 22. This produces a Qualified Electronic Timestamp under eIDAS Article 3(34), which carries legal presumption of accuracy of the date and time it indicates under eIDAS Article 41.

- Layer 3 (institution signature): the deploying operator signs the Audit Trace and the TimeStampToken. The OMP protocol implementer (Veridom or any other party implementing this profile) does not sign. This preserves evidentiary independence: the integrity claim does not depend on the continued operation, trustworthiness, or cooperation of the implementer.

The combination of these three layers satisfies the Article 12(1) tamper-resistance requirement. The Qualified Electronic Timestamp satisfies the requirement through an EU-recognised legal standard rather than a proprietary mechanism.

3.3. Requirement 3: Operational period logging

Article 12(2)(a) requires that logs capture, at minimum, the operational period of each use of the AI system.

OMP MECHANISM: Every OMP Audit Trace record includes a received_at field (ISO 8601 UTC, millisecond precision) capturing

the timestamp at which Stage S1 received the interaction, and a tst_token field containing the RFC 3161 TimeStampToken from the QTSP, which provides an externally verifiable timestamp independent of the operator's own clocks.

Under this profile, operators MUST record both timestamps. The received_at field establishes the operational period from the operator's system perspective. The tst_token provides independent temporal anchoring that does not depend on the integrity of the operator's system clock.

3.4. Requirement 4: Reference database state capture

Article 12(2)(b) requires that logs capture the reference database against which the system's input has been checked.

OMP MECHANISM: OMP computes a Source State Hash (H_s) for every external data source queried during a decision. H_s is computed as SHA-256(canonical_form(api_response) || query_timestamp_ms). This captures the exact state of the external source at the millisecond of the query. Any change to the source after the decision does not affect H_s.

Under this profile, H_s computation is MANDATORY for every external data query, including:

- Credit reference bureau queries;
- Identity verification database queries;
- Employer or educational institution verification queries;
- Any model inference API that contributes to the confidence score computation.

The H_s values are recorded in the Audit Trace source_state_hashes field (defined in Section 4.4 of this document) alongside the query timestamp and the identifier of the queried source.

3.5. Requirement 5: Input data recording

Article 12(2)(c) requires that logs capture the input data for which the system log refers, subject to applicable data protection legislation.

OMP MECHANISM: OMP normalises all interaction payloads to RFC 8785 JSON Canonicalization Scheme (JCS) [RFC8785] at Stage S1 and records the interaction_hash (SHA-256 of the canonical payload) in the Audit Trace. The canonical form is preserved in the payload_canonical field of the Interaction Schema.

Under this profile, implementations MUST record input data in canonical form to enable decision re-verification. Where the input data constitutes personal data under GDPR, operators MUST apply appropriate pseudonymisation before the payload_canonical field is committed to the Audit Trace. The interaction_hash field MUST reflect the hash of the data as actually presented to the AI system (post-pseudonymisation, if applicable), so that the canonical form can be re-verified against the pseudonymised record.

Note: The requirement to record input data is subject to Article 10 GDPR lawfulness and data minimisation requirements. Operators MUST ensure that Audit Trace records do not constitute unlawful data retention. The interaction_hash mechanism (recording a hash of the canonical payload rather than the payload itself) is designed to satisfy Article 12(2)(c) while minimising personal data retention.

3.6. Requirement 6: Decision traceability

Article 12(3) requires that, to the extent possible and technically feasible, the logging capabilities enable monitoring of the operation of the AI system with respect to the occurrence of situations that may result in risks, and to facilitate the post-market monitoring.

OMP MECHANISM: The OMP Audit Trace records, for every decision:

- The intent class and classification confidence;
- The three Confidence Score components (C_m, C_p, C_d);
- The evaluation result of every active Watchtower gate;
- The routing outcome (AUTONOMOUS, ASSISTED, or ESCALATED) with routing rationale and explicit rule reference;
- The Named Accountable Officer identity and resolution action for ASSISTED and ESCALATED outcomes.

Under this profile, the Proof-Point artefact generation mechanism (defined in [I-D.veridom-omp] Section 7.5) MUST be capable of producing a supervisory review package for any defined time window within 30 seconds of request, containing all sealed Audit Traces for that window sorted by temporal sequence, for direct submission to a Supervisory Authority upon request.

4. OMP EU AI Act Profile

4.1. Routing states under this profile

The three OMP routing states apply unchanged under this profile:

AUTONOMOUS: The AI system operates without human review for this interaction. The operator bears full accountability for the outcome. Audit Trace is generated and sealed automatically.

ASSISTED: A Named Accountable Officer reviews the AI system’s recommendation before final action. The Named Accountable Officer’s identity and decision are recorded in the Audit Trace. This state is the minimum required for interactions above the configured significance threshold.

ESCALATED: A Watchtower HARD_BLOCK has been triggered or the minimum confidence floor has not been met. Mandatory human intervention is required before the interaction can proceed. Audit Trace records the escalation reason and the Named Accountable Officer assignment.

4.2. Confidence Score configuration

Under this profile, the Confidence Score components MUST be configured as follows:

- C_p (policy compliance score): A value of 0.0 MUST force ESCALATED routing regardless of C_m or C_d values. This ensures that any detected policy non-compliance triggers mandatory human oversight, consistent with the Article 14(4) requirement for human oversight of high-risk AI systems.
- C_d (data completeness score): The minimum C_d threshold MUST be set such that decisions based on incomplete or unavailable

external data are routed to ASSISTED or ESCALATED rather than AUTONOMOUS.

4.3. Watchtower definitions

The following Watchtowers are REQUIRED under the EUAIA Profile. Operators MAY add additional Watchtowers appropriate to their specific deployment context.

WT-EUAIA-01: Fundamental Rights Impact Gate

Trigger condition: Any interaction that, if resolved AUTONOMOUS, would result in a significant effect on a natural person within the scope of Article 22 GDPR (automated individual decision-making), or where a human oversight obligation applies under Article 14 of the EU AI Act.

Action: FORCE_ASSISTED. A Named Accountable Officer MUST review the AI system’s recommendation before final action.

Rationale: Article 14(4) of the EU AI Act requires that natural persons with human oversight responsibility be able to intervene in or interrupt the functioning of the AI system. This Watchtower ensures that a human oversight opportunity exists for every interaction with potential fundamental rights implications.

WT-EUAIA-02: Significant Decision Threshold Gate

Trigger condition: Any interaction where the projected outcome exceeds an operator-configured significance threshold (examples: loan decisions above a configured value; employment decisions affecting continued engagement; educational assessments affecting qualification status).

Action: FORCE_ASSISTED.

Rationale: Ensures that high-impact individual decisions receive human oversight regardless of the AI system’s confidence score.

WT-EUAIA-03: Anomaly Detection Gate

Trigger condition: Any interaction where the AI system’s output deviates from expected operating parameters, as defined in the operator’s technical documentation under Article 11 of the EU AI Act.

Action: FORCE_ESCALATED.

Rationale: Article 12(3) requires that logging enable monitoring of situations that may result in risks. This Watchtower ensures that detected anomalies generate an escalation record with full Audit Trace, enabling post-market monitoring under Article 72.

WT-EUAIA-04: Data Quality Verification Gate

Trigger condition: Any interaction where the data completeness score C_d falls below a configured minimum, indicating that the AI system is operating with incomplete or degraded input data.

Action: FORCE_ASSISTED or FORCE_ESCALATED, depending on the severity of the data quality issue.

Rationale: Article 12(2)(b) requires that logs capture the reference database against which inputs have been checked. Where the reference database query fails or returns incomplete data, the interaction cannot be resolved AUTONOMOUS without human

review of the data quality issue.

4.4. Audit Trace schema extensions

Under the EUAIA Profile, the following fields are REQUIRED in the Audit Trace schema (in addition to the core fields defined in [I-D.veridom-omp] Section 7):

euaia_annex_iii_category (string, REQUIRED)
: The Annex III category applicable to this interaction. Example: "5b-credit-scoring" or "4-employment".

euaia_article_14_oversight (boolean, REQUIRED)
: Indicates whether the Article 14 human oversight requirement applies to this interaction. If true, WT-EUAIA-01 MUST have been evaluated.

source_state_hashes (array of objects, REQUIRED)
: An array of H_s records, one per external data source queried during this interaction. Each record MUST contain:
  - source_id (string): identifier of the queried source;
  - query_timestamp_ms (integer): Unix timestamp in milliseconds at which the query was made;
  - response_hash (string): SHA-256 of the canonical form of the API response;
  - h_s (string): SHA-256(canonical_form(response) || query_timestamp_ms).

pseudonymisation_applied (boolean, REQUIRED)
: Indicates whether pseudonymisation was applied to personal data before payload_canonical was committed to the Audit Trace. If true, the interaction_hash reflects the hash of the pseudonymised payload.

proof_point_version (string, REQUIRED)
: Semantic version of the EUAIA Profile specification under which this Audit Trace was generated. MUST be set to "VERIDOM-EUAIA-v1.0" for this profile version.

supervisory_authority_jurisdiction (string, REQUIRED)
: The ISO 3166-1 alpha-2 country code of the EU Member State whose designated Supervisory Authority has jurisdiction over this deployment. Example: "DE", "FR", "NL".

5. eIDAS Legal Framework Alignment

The OMP three-layer integrity architecture produces a Qualified Electronic Timestamp under eIDAS when the RFC 3161 TimeStampToken is issued by a QTSP listed in an EU Member State trusted list.

The legal significance of this alignment is precise:

- eIDAS Article 41(1) establishes legal presumption of the accuracy of the date and time a Qualified Electronic Timestamp indicates and the integrity of the data to which the date and time are bound.

- This legal presumption applies in legal proceedings in all EU Member States under Article 41(2).

- A Supervisory Authority examining an OMP Audit Trace sealed with a Qualified Electronic Timestamp receives an evidence record with statutory presumption of integrity and temporal accuracy.

Regulation (EU) No 910/2014 on electronic identification and

trust services (eIDAS) [EIDAS]

Under this profile, implementations MUST use a QTSP that is listed in an EU Member State trusted list maintained under Article 22 of eIDAS. Acceptable QTSPs include DigiCert EU (DE), GlobalSign (BE), and Actalis (IT), among others listed at esignature.ec.europa.eu/tl-browser.

Implementations MAY use a non-EU TSA for development or testing purposes, but production deployments under this profile MUST use a QTSP.

6. Annex III Category Mapping

The following table maps the primary Annex III categories of the EU AI Act to the applicable Watchtower configurations and the OMP domain profiles that should be used in conjunction with this profile.

Category 5(b) -- Credit scoring and creditworthiness:
Required Watchtowers: WT-EUAIA-01, WT-EUAIA-02, WT-EUAIA-04.
Complementary profile: [I-D.veridom-omp-ndtcp] for Kenya deployments.

Category 4 -- Employment and worker management:
Required Watchtowers: WT-EUAIA-01, WT-EUAIA-02, WT-EUAIA-03.
Rationale: Employment decisions have high fundamental rights impact; anomaly detection is particularly important for automated hiring or performance management systems.

Category 3 -- Education and vocational training:
Required Watchtowers: WT-EUAIA-01, WT-EUAIA-02.

Category 8 -- Administration of justice:
Required Watchtowers: WT-EUAIA-01, WT-EUAIA-02, WT-EUAIA-03.
Complementary profile: a forthcoming OMP legal domain profile for ABA Rule 5.3 / CA SB 574 deployments.

For categories not listed above, operators MUST apply at minimum WT-EUAIA-01 and WT-EUAIA-04, and SHOULD apply WT-EUAIA-02 for any interaction with individual-level consequences.

7. Conformity Assessment

Operators deploying OMP under this profile who are subject to the Article 43 conformity assessment requirement may present the following evidence to a Notified Body or in a self-assessment under Article 43(4):

- The OMP Technical Specification [ZENODO-OMP] as the reference technical documentation for the logging and traceability mechanism;
- The IETF Internet-Draft [I-D.veridom-omp] as evidence of the open, publicly reviewed specification of the cryptographic sealing architecture;
- A sample Audit Trace record sealed under this profile, together with the output of the OMP Reference Validator [OMP-OPEN-CORE], demonstrating chain integrity and Qualified Electronic Timestamp authenticity;
- The operator’s domain-specific Watchtower configuration, demonstrating that WT-EUAIA-01 through WT-EUAIA-04 are implemented as required.

The OMP Reference Validator is published as open-source software under the Apache 2.0 licence at [OMP-OPEN-CORE]. Any Notified Body, Supervisory Authority, or third-party auditor may run the Reference Validator against any OMP Audit Trace chain without access to the operator's infrastructure or Veridom's systems.

8. Security Considerations

The security considerations of [I-D.veridom-omp] apply in full to this profile. The following additional considerations apply to EU AI Act deployments.

Key management: Operators MUST implement appropriate key management practices for the institution signature private key, consistent with eIDAS Annex II requirements for advanced electronic signatures. Compromise of the institution signature private key does not invalidate historical Audit Traces, whose integrity is anchored by the QTSP TimeStampToken, but would allow fabrication of future records attributed to the institution.

GDPR interaction: Audit Trace records that contain or are associated with personal data are subject to GDPR data retention and erasure requirements. Operators MUST implement a mechanism for satisfying Article 17 GDPR erasure requests in a manner consistent with the chain integrity properties of the Merkle structure. Recommended approach: selective pseudonymisation of personal data fields in historical records, with a public record of the pseudonymisation event in the chain, rather than deletion of the Audit Trace record itself.

Supervisory access: Operators MUST be capable of producing the full Audit Trace chain for any deployment period to the designated Supervisory Authority within the timeframes specified by national implementing legislation. The Proof-Point artefact generation mechanism (Section 3.6) is designed to support this capability.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. Normative References

[I-D.veridom-omp] Adebayo, T., Apalowo, O., and F. Makanjuola, "Operating Model Protocol (OMP): A Deterministic Decision-Enforcement Protocol with Externalized Proof-of-Integrity", draft-veridom-omp-00 (work in progress), March 2026.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785,

June 2020.

10.2. Informative References

[EUAIA] European Parliament and of the Council, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", Official Journal of the European Union, July 2024.

[EIDAS] European Parliament and of the Council, "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market", Official Journal of the European Union, August 2014.

[I-D.veridom-omp-ndtcp] Adebayo, T., Apalowo, O., and F. Makanjuola, "OMP Domain Profile: Kenya Digital Credit Providers -- CBK NDTCP Regulations 2022", draft-veridom-omp-ndtcp-00 (work in progress), March 2026.

[OMP-OPEN-CORE] Veridom Ltd, "OMP Open Core: Reference Validator and Schema Library", Apache 2.0, https://github.com/veridomltd/omp-open-core, 2026.

[ZENODO-OMP] Adebayo, T., Apalowo, O., and F. Makanjuola, "OMP -- Operating Model Protocol: A Deterministic Routing Invariant for Tamper-Evident AI Decision Accountability in Regulated Industries", Zenodo, DOI 10.5281/zenodo.19140948, March 2026.

Authors' Addresses

Tolulope Adebayo
Veridom Ltd
London, United Kingdom
Email: tolulope@veridom.io

Oluropo Apalowo
Veridom Ltd
Awka, Nigeria
Email: ropo@veridom.io

Festus Makanjuola
Veridom Ltd
Toronto, Canada
Email: festus@veridom.io